CLAIMS

What is claimed is:

1. A user authentication method comprising:

obtaining a user identification (ID) recognizable by an enterprise access management (EAM) system;

generating a login request based upon said user ID, said login request being void of a user password corresponding to said user ID; and

evaluating said login request with a processing module compatible with said EAM system.

2. A method according to claim 1, wherein said evaluating step comprises determining whether said login request was generated by a trusted source.

3. A method according to claim 1, wherein said evaluating step comprises validating said user ID.

4. A method according to claim 3, further comprising said EAM system performing an access management action if said validating step validates said user ID.

5. A method according to claim 1, wherein said user ID represents a user authenticated by a system independent of said EAM system.

6. A user authentication method comprising:

obtaining a user identification (ID) recognizable by an enterprise access management (EAM) system;

creating an encrypted expression based upon said user ID; and

sending said encrypted expression to a processing module compatible with said EAM system.

7. A method according to claim 6, further comprising generating a login request that includes said encrypted expression.

8. A method according to claim 7, wherein said encrypted expression is sent to said processing module with said login request.

9. A method according to claim 7, wherein said login request is void of a user password corresponding to said user ID.

10. A method according to claim 6, wherein said creating step encrypts a hash to create said encrypted expression.

11. A method according to claim 10, further comprising performing a hashing operation on a string to compute said hash, wherein said string is based upon said user ID.

12. A user authentication method comprising:

receiving a login request at a processing module compatible with an enterprise access management (EAM) system, said login request including a user identification (ID) recognizable by said EAM system, and said login request being void of a user password corresponding to said user ID; and

said processing module evaluating said login request to determine whether said login request was generated by a trusted source.

13. A method according to claim 12, further comprising generating a parameter based upon user ID.

14. A method according to claim 13, further comprising performing a hashing operation on said parameter to compute a hash.

15. A method according to claim 14, further comprising:

encrypting said hash to create a first encrypted expression;

extracting a second encrypted expression from said parameter; and

comparing said first encrypted expression to said second encrypted expression.

16. A method according to claim 15, further comprising validating said login request if said comparing step results in a match between said first encrypted expression and said second encrypted expression.

17. A method according to claim 16, further comprising said EAM system performing an access management action if said validating step validates said login request.

18. A method according to claim 14, further comprising:

extracting an encrypted expression from said parameter;

decrypting said encrypted expression to obtain a second hash; and

comparing said hash to said second hash.

19. A method according to claim 18, further comprising validating said login request if said comparing step results in a match between said hash and said second hash.

20. A method according to claim 19, further comprising said EAM system performing an access management action if said validating step validates said user ID.

21. A user authentication method comprising:

obtaining a user identification (ID) recognizable by an enterprise access management (EAM) system;

forming a string based upon said user ID and an identifier;

performing a hashing operation on said string to compute a hash;

encrypting said hash, with an encryption algorithm that utilizes a key corresponding to said identifier, to create an encrypted expression; and

generating a login request that includes said user ID and a parameter derived from said encrypted expression, said login request being void of a user password corresponding to said user ID.

22. A method according to claim 21, wherein said encrypting step utilizes a symmetric encryption algorithm.

23. A method according to claim 21, wherein said string is formed as a concatenation of said user ID and said identifier.

24. A method according to claim 21, further comprising receiving said login request at a processing module compatible with said EAM system.

25. A method according to claim 24, further comprising said processing module:

generating said string from parameters included with said login request; and

performing said hashing operation on said string to compute a second hash.

26. A method according to claim 25, further comprising said processing module:

extracting said identifier from said login request;

retrieving a stored key corresponding to said identifier; and

encrypting said second hash, with an encryption algorithm that utilizes said stored key, to create a second encrypted expression.

27. A method according to claim 26, further comprising said processing module:

extracting said encrypted expression from said login request;

comparing said encrypted expression to said second encrypted expression; and

validating said login request if said comparing step results in a match between said first encrypted expression and said second encrypted expression.

28. A method according to claim 25, further comprising said processing module:

extracting said identifier and said encrypted expression from said login request;

retrieving a stored key corresponding to said identifier; and

decrypting said encrypted expression, with a decryption algorithm that utilizes said stored key, to obtain a decrypted expression.

29. A method according to claim 28, further comprising said processing module:

comparing said second hash to said decrypted expression; and

validating said login request if said comparing step results in a match between said second hash and said decrypted expression.

30. A computer program embodied on a computer-readable medium, said computer program having computer-executable instructions for carrying out a method comprising:

obtaining a user identification (ID) recognizable by an enterprise access management (EAM) system;

creating an encrypted expression based upon said user ID; and

sending said encrypted expression to a processing module compatible with said EAM system.

31. A computer program embodied on a computer-readable medium, said computer program having computer-executable instructions for carrying out a method at a processing module compatible with an enterprise access management (EAM) system, said method comprising:

receiving a login request including a user identification (ID) recognizable by said EAM system, said login request being void of a user password corresponding to said user ID; and

evaluating said login request to determine whether said login request was generated by a trusted source.